Enhanced Security using RSA Algorithm in Cloud Computing

Dr. Sonia Sharma [1], Ashutosh Kumar [2]

[1]Professor & Head, Department of Computer Science and Engineering, MIMIT Malout

[2]Research Scholar, Department of Computer Science and Engineering, MIMIT Malout

Abstract: The cloud computing has a very important aspect i.e., the security and the quality of service from cloud service providers. However, cloud computing poses many new security challenges which haven't been well investigated. This paper specializes the issues referring to the cloud data storage methods and security within the virtual environment. In this paper, a technique for suggesting data storage and security within the cloud system using combination of public-key and private-key cryptosystem RSA has been implemented [5]. Further, it describes the safety services includes key generation, encryption and decryption within the virtual environment.

Keywords— RSA algorithm, encoding, Cloud Computing, Data Security, Data Decryption

I. Introduction

In the modern distributed era various services offered on the web are a standard hosting system. But within the normal hosting system storage and usage are fixed. Cloud computing imposes a replacement model for computing and the issues like compute, storage, software. A development environment is being provided and the allocation and reallocation of resources is completed wherever storage is needed and virtualized it. It satisfies the on-demand needs of the user. For the organization, the cloud offers data centres to maneuverer their data globally. It removes the usages of local nodes for supporting their data and also cloud supports upgradable resources on the net. Cloud Service Providers maintains Computing resources and data automatically via software [6]. Cloud Computing is that the key thrust in many companies but the key concern is the safety of their data within the cloud. Securing data is sometimes of being vital due to the critical nature of cloud. Henceforth, the priority regarding data privacy and security are solving a barrier to the broader the upgrade of cloud computing services. Data Security must be imposed on data by using encryption strategies to understand secured data storage and access. The cloud infrastructure is even more reliable and powerful than personal computing, but an oversized range of internal, external threats for data stored. Since the information don't seem to be stored within the client area, implementing security measures can't be applied directly. During this work, the RSA algorithm is implemented before storing sensitive data within the cloud. [1] When the authorized user requests the information for usage then data decrypted and provided to the user. In this paper, a way for Cloud ADPS by providing data storage and securing Cloud automatic processing system using RSA algorithm [8] and some important security services including key generation, encryption and decryption are provided in Cloud automatic data processing has been proposed.

II. Cloud Computing

Cloud computing is an emerging paradigm, which mainly concentrates to supply dynamic, on-demand scalability of virtualized recourse to line of users. Scalability and virtualization are the two key factors

of the cloud environment. because of the accessibility of the cloud computing services many researchers are focus on this area.

III. Cloud Architecture and Storage Architecture—

A. *Cloud Architecture*: It typically involves multiple cloud components communicating with one another over application programming interfaces, usually web services. This is reverted to the clients where cloud applications can be accessed by software applications or web.

B. *Cloud Storage Architecture*: High-level architecture description of cloud data storage services illustrated in Fig. 1. The architecture consists of 4 different entities: data owner, user, cloud server (CS), and Third-party Auditor (TPA) [7]. The access of cloud storage security behalf of user, TPA is the trusted entity.

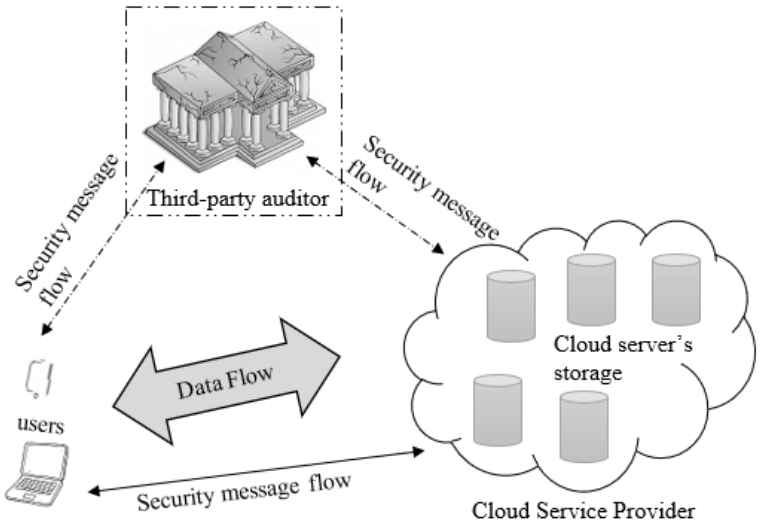

Fig. 1. The given is a sample model of cloud architecture which defines a cloud storage and infrastructure being using its services and the flow of data through the servers.

IV. Cloud Computing Service and Deployment Models

a. Service Models

Cloud computing separated into three service categories:

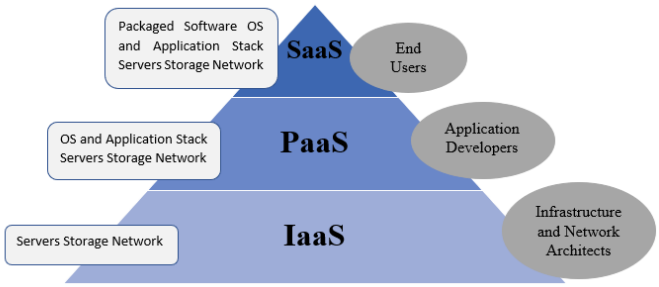

Fig. 2. The given is the service model description of cloud and their application.

Infrastructure as a service (IaaS) is a part of cloud computing resources that is virtualized. The hardware, software, servers, storage and other infrastructure components in IaaS are being hosted by a third-party provider on behalf of their users. Users' applications are also being provided by IaaS and handles tasks covering system maintenance backup and resiliency planning. IAAS platforms offer

highly scalable resources that can be adjusted on-demand to make it working for workloads that are temporary, experimental or changed unexpectedly. Other characteristics of IAAS environments covers dynamic scaling, desktop virtualization, the automation of administrative tasks and policy-based services. [3]

Platform as a service (PaaS) is also a cloud computing model that delivers applications. During a PaaS model, cloud provider delivers hardware and software tools i.e., being hosted by its own infrastructure. Actually, they are used for the application development as a service for users. Hence it leads to freeing PaaS users from putting in place in-house hardware and software to develop or run a replacement application. A PAAS provider, however, supports all the underlying computing and software; users only must login and start using the platform-usually through a web browser interface. [4] PAAS providers then charge for that access on a per-use basis or monthly basis.

Software as a service (SaaS) is a part of software distribution model from where applications are hosted by service provider and made available online for the customers [2]. SAAS has become an increasingly prevalent delivery model as underlying technologies that support Web services and service-oriented architecture (SOA) mature and new development approaches, like Ajax, become popular. SAAS is very similar to the ASP (Application service provider) and on-demand computing software delivery models. IDC identifies two minimal difference in delivery models for SAAS namely the hosted application model and so the software development model.

b. Deployment Models

i. **Private cloud**: During this model cloud owner doesn't share their resources with the other organization. it's founded and maintained by a company. Security is often fine implemented during this model.
ii. **Public cloud**: During this cloud model the resources are accessed by the final public. Everybody can access easily with this cloud so it's a less secure model. Cost of this cloud isn't expensive. This model requires a large investment these are owned by large organizations like Microsoft, Google or Amazon.
iii. **Community cloud**: A cloud shares two or more several organizations or companies for his or her requirements. Usually employed in school or university campus.
iv. **Hybrid cloud**: This sort of cloud uses one or more cloud model combinations for better use.

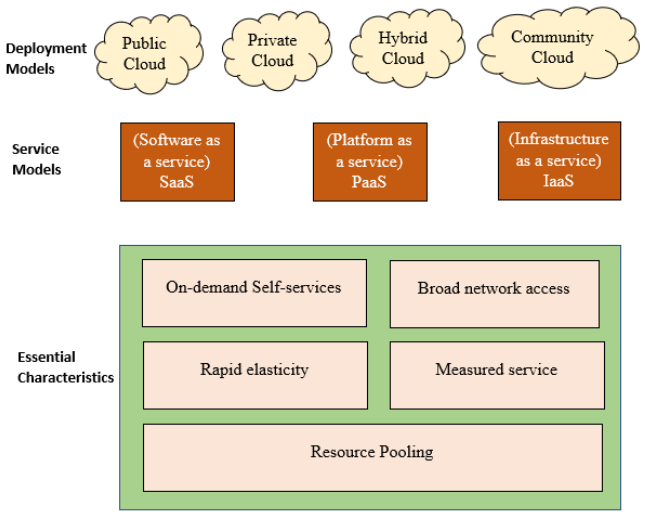

Fig. 3. Cloud model showing the composition of various service models and deployment models

V. The Proposed Methodology

The area of cryptography and cryptanalysis together are referred to as cryptology. Cryptanalysis used many encryptions and decryption techniques like Caeser cipher, Monoalphabetic cipher, Play fair cipher, Hill Cipher. These techniques possess the Brute Force Attack means the attacker tries every possible key to induce the first text to avoid this problem public key cryptography used. RSA is widely used Public-Key algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977.[9]

In this proposed work, it is used for RSA algorithm to encrypt the information to produce security in order that only the concerned user can access it by securing the info as well as cipher.

RSA algorithm is that the public-key cryptography, within which both public and also the private keys are accustomed secure data within the cloud. the event of the general public key cryptography is greatest and maybe it provides a radical departure. it's also referred to as the Asymmetric algorithm because of the employment of two key together with a secret key. during this scheme, the plain text and cipher text are integers between 0 and n-1 for a few n. A typical size for n is 1024 bits. [3]

RSA is a block cipher during which every message is mapped to an integer. RSA consists of Public-Key and Private-Key [1]. In this Cloud environment, Pubic-Key is understood to any or all, whereas Private-Key and encrypted cipher key is thought only to the user who originally owns the info [10]. Thus, encryption is finished by the Cloud service provider and decryption is finished by the Cloud user or consumer.

Once the information is encrypted with the Public-Key, it may be decrypted with the corresponding Private-Key only.

RSA algorithm involves three steps:

- Key Generation
- Encryption
- Decryption

Key generation: Before the information is encrypted Key generation should be done. This process is finished between the Cloud service provider and therefore the user. [2]

Key generation algorithm Steps:

1. Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.
2. Compute n = a * b.
3. Compute Euler's totient function,
   Ø(n) = (a-1) * (b-1).
4. Chose an integer e, such that 1 < e < Ø(n) and a greatest common divisor of e, Ø(n) are 1.
   Now, e is released as Public-Key exponent.
5. Now determine d as follows:
   $d = e^{-1}$ (mod Ø(n)) i.e., d is multiplicate inverse of e mod Ø(n).
6. d is kept as Private-Key component, so that d * e = 1 mod Ø(n).
7. The Public-Key consists of modulus n and the public exponent e i.e, (e, n).
8. The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e., (d, n).

Encryption algorithm: Encryption is the process of converting original plain text (data) into cipher text (data). [9]

Steps:

1. The cloud service provider should give or transmit the Public- Key (n, e) to the user who wants to store the data with him or her.
2. User data is now mapped to an integer by using an agreed-upon reversible protocol, known as padding scheme.
3. Data is encrypted and the resultant cipher text(data) C is $C = m^e \pmod n$.
4. This cipher text or encrypted data is now encrypted again with the key (n, e) and being stored with the Cloud service provider.

Decryption algorithm:

Decryption is the process of converting the cipher text(data) to the original plain text(data). [3]

Steps:

1. The cloud user requests the Cloud service provider for the data.
2. Cloud service provider verifies the authenticity of the user and gives the encrypted cipher i.e., cipher.
3. The Cloud user then decrypts the cipher using values (d, n) first and hence the data by computing, $m = C^d \pmod n$.
4. Once m is obtained, the user can get back the original data by reversing the padding scheme.

VI. Experimental results and analysis

One of the experimental results shown here with the sequence of sections.

Key generation part:

The first part of key generation is to encrypt the original message into some integral byte code.

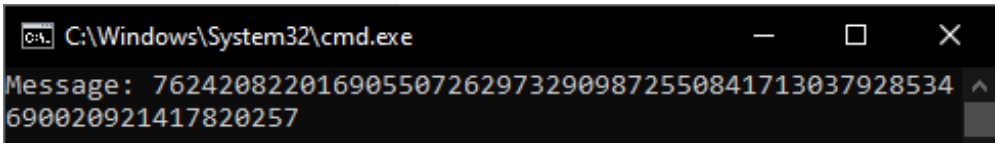

Fig. 4. Encrypted data

After the encryption of the message, two prime numbers are being chosen randomly to avoid the complication of attacking. Once the prime number is selected, p1*p2 is calculated according to the algorithm of RSA. Hence Euler's Totient is computed.

Fig. 5. Generation of random prime numbers and calculating values for keys

Encryption part:

The generation of public key and private key from the cipher generated by encrypting message. These keys emerged from the prime numbers chosen and the value generated as e, n ,d.

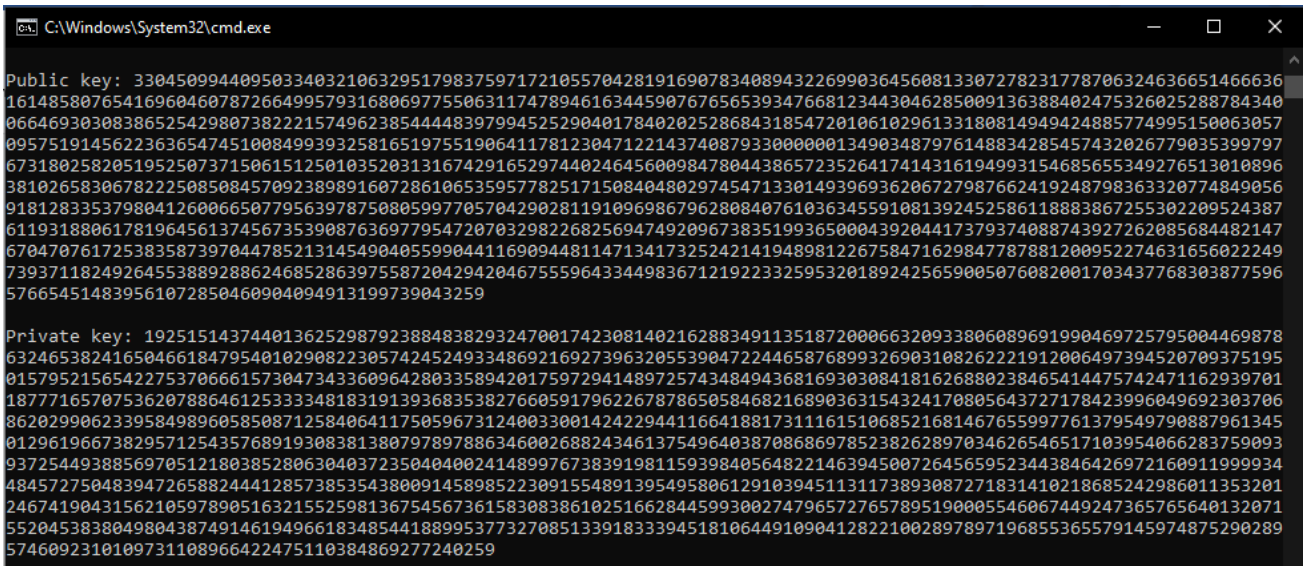

Fig. 6. Generated private and public key component

The encrypted cipher which is being used further in decryption part for the decryption of the cipher so that the original data can be retrieved.

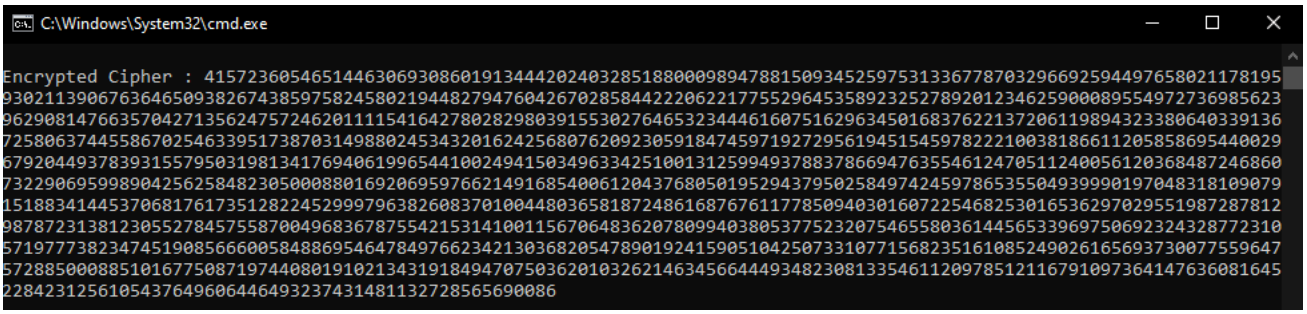

Fig. 7. Encrypted Cipher

Decryption part:

Finally, the data is being decrypted using the key and the cipher text.

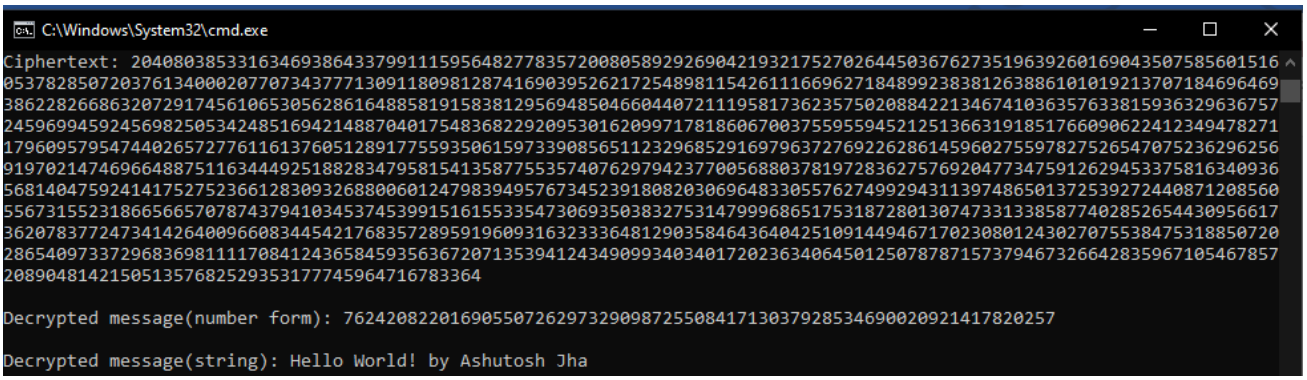

Fig. 8. Decrypted cipher text and hence the data decrypted

VII. Conclusion

Cloud Computing remains a replacement and evolving paradigm where computing is thought to be on-demand service. Once the organization decides to maneuverer to the cloud, it loses control over the info. Thus, the quantity of protection needed to secure data is directly proportional to the worth of the information. Cloud Security basically depends on the trusted computing and cryptography. Thus, in this proposed work, only the authorized user can access the information. whether or not some intruder (unauthorized user) gets the info accidentally or intentionally if he/she captures the info also, he/she can't decrypt it and obtain back the initial data from it. Henceforth, data security is provided by implementing the RSA algorithm. In this work, performance supported different parameters like space complexity, time complexity and throughput has been observed. we've got observed each efficiency parameter intimately by varying message packet length and a non-public key length of our encryption scheme. On viewing the results, it good to say that the RSA encryption algorithm is a feasible solution for secure communication in cloud computing.

References—

[1] Shreya Srivastav, Shalika "Improving data security in cloud computing by using RSA and Digital Signature Algorithm "A special issue ofIJTR(ISSN 2278-5787) SERB sponsored two day national conference on " Current trends in scientific research for engineering applications (NCCSE-2015)" dated march 20-21, 2015

[2] P.suresh "Secure Cloud Environment Using Rsa Algorithm", International Journal of Computer Science and Information Technology, e-ISSN: 2395 -0056, p-ISSN: 2395-0072, Volume: 03 Issue: 02 | Feb-2016

[3] Santosh Kumar Singh, Dr. P.K. Manjhi, Dr. R.K. Tiwari, "Data Security using RSA Algorithm in Cloud Computing", International Journal of Advanced Research in Computer and Communication Engineering, ISSN (Online) 2278-1021, Vol. 5, Issue 8, August 2016.

[4] Sudhansu Ranjan Lenka, Biswaranjan Nayak, International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, June-2014

[5] Dr. Rajamohan Parthasarathy, Ms. Haw Wai Yee P, Mr. Seow Soon Loong, Dr. Leelavathi Rajamanickam, Ms. Preethy Ayyappan, IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 6 Issue 4, April 2019, ISSN (Online) 2348 – 7968

[6] Dhaval Jha Vishva Tanna Ripal Patel, " Data Security in Cloud using RSA" - International Journal for Scientific Research & Development| Vol. 2, Issue 04, 2014 | ISSN (online): 2321-0613

[7] Shreya Srivastav, Neeraj Verma, M. Tech Scholar, Department of CSE, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 7, July 2015

[8] Ms. Soumya.N.S, Mrs. Prabha.R, M.Tech Student, Computer Network Engineering, Associate Professor, Department of Information Technology, Volume IV, Issue X, October 2015 IJLTEMAS ISSN 2278 – 2540

[9] Nasrin Khanezaei, Zurina Mohd Hanapi, "A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services", IEEE, 58-62, 2014.

[10] Balkees Mohamed Shereek, ZaitonMuda, SharifahYasin, Faculty of computer science and information technology, IOSR Journal of Engineering (IOSRJEN)ISSN (e): 2250-3021, ISSN (p): 2278-8719 Vol. 04, Issue 02 (February. 2014), ||V6|| PP 01-08